


AUTHENTICATION METHOD FOR CONNECTION ESTABLISHMENT BETWEEN DEVICES

Patent number:	KR2001051049
Publication date:	2001-06-25
Inventor:	PARK JAE HAN (KR)
Applicant:	SAMSUNG ELECTRONICS CO LTD (KR)
Classification:	
- international:	H04L9/32
- european:	
Application number:	KR20000060702 20001016
Priority number(s):	KR19990052658 19991125

Also published as:

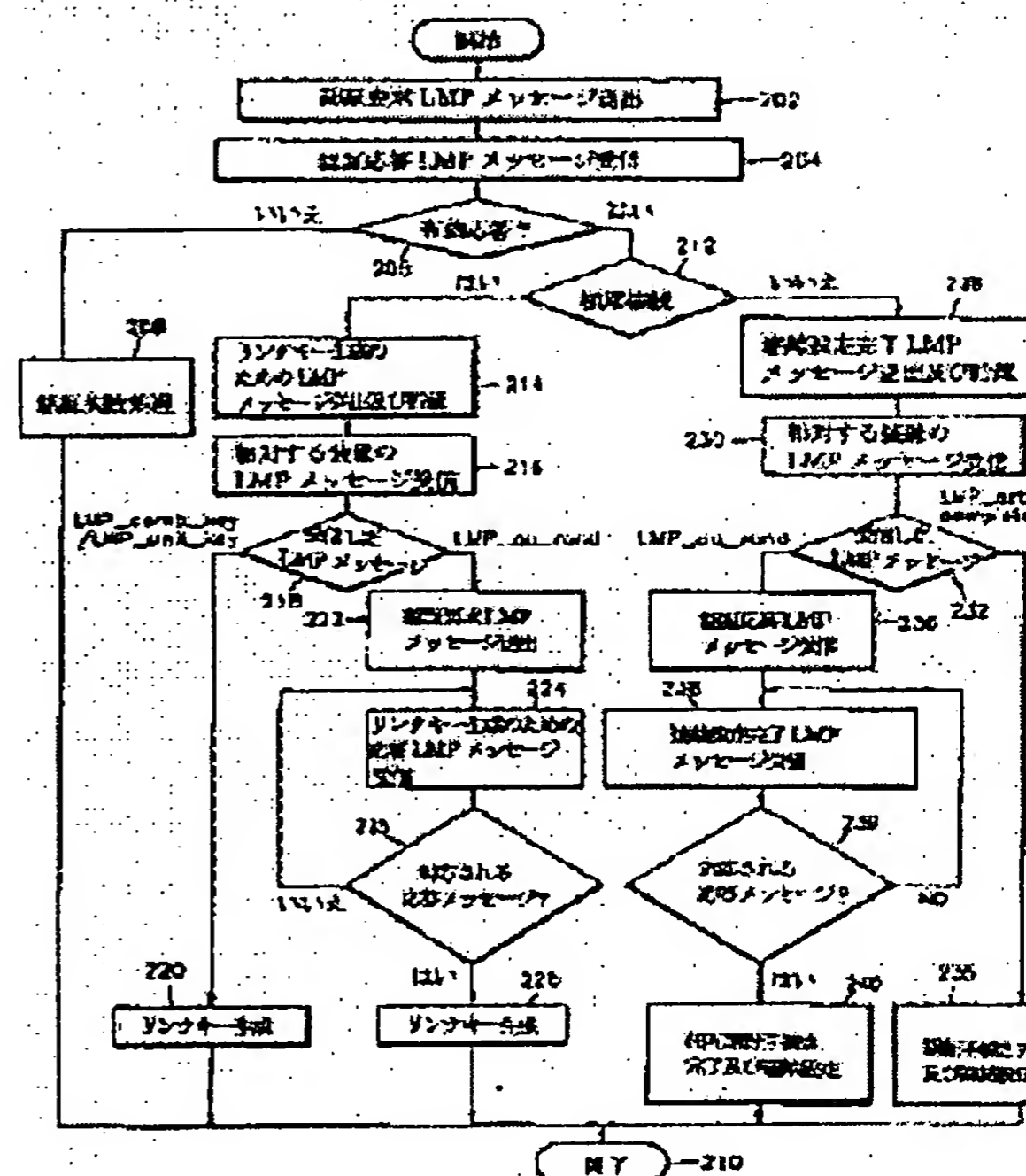
 JP2001223692 (A)

Report a data error here

Abstract not available for KR2001051049
Abstract of corresponding document: JP2001223692

PROBLEM TO BE SOLVED: To provide an authentication method to set connection between devices desiring data transmission reception under a communication environment using communication standards, such as Bluetooth.

SOLUTION: The method is configured, such that the authentication procedure to set connection between devices desiring data transmission reception is decided for a single authentication procedure or a mutual authentication procedure, on the basis of the authentication condition set to a device receiving an authentication request in devices that transmit/receive data. Thus, the setting of connection between the devices going to send/receive data under a communication environment operated, on the basis of the communication standards, such as Bluetooth, can be conducted more reliably and accurately.



Data supplied from the *esp@cenet* database - Worldwide

공개특허특2001-0051049

(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl. 6
H04L 9/32

(11) 공개번호 특2001-0051049
(43) 공개일자 2001년06월25일

(21) 출원번호 10-2000-0060702

(22) 출원일자 2000년10월16일

(30) 우선권 주장 10199900526581999년11월25일대한민국(KR)

(71) 출원인 삼성전자 주식회사 윤종용
경기 수원시 팔달구 매탄3동 416

(72) 발명자 박재한
경기도용인시기흥읍서천리163-7리빙타운305호

(74) 대리인 이영필
최홍수
이해영

심사청구 : 없음

(54) 장치간의 연결 설정을 위한 인증방법

요약

본 발명은 블루투스(Bluetooth)와 같은 통신 규격을 이용하는 통신환경에 있어서, 데이터 송수신을 원하는 장치간의 연결을 설정하기 위한 인증방법을 개시한다. 본 발명에 따른 방법은, 데이터를 송수신할 수 있는 장치 중 인증 요구를 수신하는 장치에 설정되어 있는 인증조건에 따라 데이터 송수신을 원하는 장치간의 연결 설정을 위한 인증절차를 단일 인증절차로 수행할 것인지 상호 인증절차로 수행할 것인지를 결정하여 수행하도록 구성된다. 따라서, 블루투스와 같은 통신 규격을 토대로 운영되는 통신 환경에서 데이터를 송수신하고자 하는 장치간의 연결 설정을 좀더 신뢰성 있고 정확하게 할 수 있다.

대표도

도2

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 방법을 수행하기 위한 장치의 기능 블록도이다.

도 2A,B는 본 발명에 따른 인증방법을 수행하는데 있어서 인증 요구 개시측의 동작 흐름도이다.

도 3A, B는 본 발명에 따른 인증방법을 수행하는데 있어서 인증요구 수신측의 동작 흐름도이다.

도 4A, B는 초기 접속 단계에서의 인증 절차도이다.

도 5A, B는 링크 키가 설정된 후의 인증 절차도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야 종래기술

본 발명은 데이터 송수신이 가능한 장치(device)간의 연결(connection)을 설정(establishment)하기 위한 인증방법에 관한 것으로, 특히, 블루투스(Bluetooth)와 같은 통신 규격을 이용하는 통신환경에서 데이터 송수신을 원하는 장치간의 연결 설정을 위한 인증(authentication) 방법에 관한 것이다.

블루투스는 물리적인 케이블(cable)없이 무선주파수(radio frequency, RF)를 이용하여 각종 전자기기(electronic devices)간에 고속으로 데이터 송수신을 가능하게 하는 것으로, 근접 무선 데이터 통신 규격(local wireless data communication specification)이다. 이 블루투스는 음성 부호화방식의 CVSD(Continuous Variable Slope Delta Modulation)를 채용하여 공간의 제한 없이 문자 데이터는 물론이고 음성 전송도 가능하다.

이러한 블루투스와 같은 통신 규격을 이용하는 통신환경에서 데이터를 송수신하기 위한 장치들은 데이터를 송수신하기 전에 원하는 장치간에 연결(connection)이 설정되어야 한다. 연결을 설정하는 과정은 크게 RF동기를 맞추는 과정, 통신하고자 하는 장치의 링크 관리자간의 링크 설정과정 및 채널설정과정으로 구분될 수 있다. 그러나, 아직까지 블루투스와 같은 통신 규격을 이용하는 통신환경에 대한 규격 제정이 완벽하게 이루어지지 않았기 때문에 상술한 연결과정을 비롯한 여러 부분에서 해당되는 규정 제정을 위한 연구가 다각도로 진행되고 있다.

발명이 이루고자하는 기술적 과제

따라서 본 발명은 블루투스와 같은 통신 규격을 이용하는 통신환경에 있어서, 데이터 송수신을 원하는 장치간의 연결을 설정하기 위한 인증방법을 제공하는데 그 목적이 있다.

본 발명의 다른 목적은 블루투스와 같은 통신 규격을 이용하는 통신환경에 있어서, 데이터 송수신을 원하는 상대 장치의 인증조건에 따라 데이터 송수신을 원하는 장치간의 연결을 설정하기 위한 인증절차를 수행하는 인증방법을 제공하는데 있다.

발명의 구성 및 작용

상기 목적들을 달성하기 위하여 본 발명에 따른 방법은, 무선으로 데이터를 송수신할 수 있는 장치간의 연결을 설정하기 위한 인증 방법에 있어서, (a) 연결 설정을 원하는 상대 장치와의 인증절차를 수행하기 위해 상대 장치측으로 제 1 인증요구 메시지를 송출하는 단계;(b) 제 1 인증요구 메시지에 대한 인증 응답 메시지가 수신되면, 현재의 동작모드에 따른 소정의 메시지를 상대 장치로 송출하면서 저장하는 단계;(c) (b)단계 수행 후, 상대 장치로부터 제 1 메시지가 수신되면, 제 1 메시지가 소정의 메시지에 대응되는 응답 메시지인지를 체크하는 단계;(d) (c)단계의 체크결과, 제 1 메시지가 응답 메시지가 아니고, 제 2 인증요구 메시지이면, 제 2 인증요구 메시지에 대응되는 응답 메시지를 상기 상대 장치로 송출하는 단계; (e) (d)단계 수행 후, 상대 장치로부터 제 2 메시지가 수신되면, 제 2 메시지가 소정의 메시지에 대응되는 응답 메시지인지를 체크하는 단계;(f) (e)단계 체크결과, 제 2 메시지가 소정의 메시지에 대응되는 응답 메시지이면, 인증절차를 완료하는 단계를 포함하는 것이 바람직하다.

상기 목적들을 달성하기 위하여 본 발명에 따른 방법은, 무선으로 데이터를 송수신할 수 있는 장치간의 연결을 설정하기 위한 인증 방법에 있어서, (a) 연결 설정을 원하는 상대 장치로부터 인증 절차를 수행하기 위한 제 1 인증요구 메시지가 수신되면, 제 1 인증요구 메시지에 대응되는 응답 메시지를 송출하는 단계;(b) (a)단계 수행 후, 상대 장치로부터 소정의 메시지가 수신되면, 자신의 인증 조건을 체크하는 단계;(c) 자신의 인증 조건을 체크한 결과, 상호 인증이 필요하면, 소정의 메시지를 저장하고, 제 2 인증요구 메시지를 상대 장치로 송출하는 단계;(d) (c)단계 수행 후, 상대 장치로부터 제 2 인증요구 메시지에 대응되는 응답 메시지가 수신되면, (c)단계에서 저장한 메시지에 대응되는 응답 메시지를 상대 장치로 송출하면서 인증 절차를 완료하는 단계를 포함하는 것이 바람직하다.

이하, 첨부된 도면을 참조하여 본 발명을 상세히 설명한다.

도 1은 본 발명에 따른 인증방법을 수행하기 위한 시스템의 기능 블록도이다. 도 1을 참조하면, 상술한 시스템은, 인증요구 개시측(100)과 인증요구 수신측(110)으로 구성된다. 인증요구 개시측(100)과 인증요구 수신측(110)은 각각 블루투스와 같은 통신 규격으로 데이터를 송수신할 수 있는 서로 다른 장치에 구비된다. 예를 들어, 인증요구 개시측(100)은 발신측에 해당되는 장치에 구비되고, 인증요구 수신측(110)은 착신측에 해당되는 장치에 구비된다. 이러한 인증요구 개시측(100)과 인증요구 수신측(110)은 각각 호스트 제어 인터페이스부(Host Controller Interface)(102)(112), 링크 관리자(Link Manager)(106)(116), 종단부(end portion)(108)(118)를 각각 포함한다. 링크 관리자들(106)(116)은 각각 메모리(105, 115)를 포함한다.

호스트 제어 인터페이스부(102)(112)는 각각 대응되는 호스트(미 도시됨)와 데이터 송수신을 하기 위한 것으로, 레이어 2(layer 2)에 해당되는 정합처리(interface)를 수행한다. 도 1은 인증요구 개시측(100)과 인증요구 수신측(110)이 해당되는 호스트(미 도시됨)와 분리된 경우를 도시한 것이다. 호스트(미 도시됨)는 광의적으로 블루투스과 같은 통신 규격에 따라 운영되는 하나의 장치이고, 협의적으로 여러 가지 기능들을 갖춘 장치의 중앙제어부(미 도시됨)에 의해 제어되어 블루투스과 같은 통신 규격에 따른 모드에서 동작되도록 상술한 장치 내에 설치된 하나의 모듈이다. 이 호스트(미 도시됨)는, 호스트 제어 인터페이스부(102)(112)와의 연결(connection)을 위한 채널을 설정하기 위하여, 레이어 2에 해당되는 기능을 수행하는 L2 CAP(Logical Link Control and Adaptation Protocol) 및 응용(Application)기능 등을 수행하도록 구현된다.

링크 관리자(106)(116)는 블루투스과 같은 통신 규약에 따라 데이터 송수신을 원하는 장치와의 연결을 설정 및 해제(connection establishment/release)하고, 연결이 설정되면 해당되는 장치의 링크 관리자(116)(106)간에 형성된 링크를 운영(handling)하는 기능을 수행하도록 구현된다. 특히, 메모리(105)(115)는 해당되는 장치간의 연결을 설정하기 위해 필요한 링크 관리 프로토콜(Link Management Protocol, 이하 LMP라고 약함) 메시지를 저장한다.

종단부(108)(118)는 데이터 송수신을 위한 고주파 처리와 베이스 밴드(Baseband) 제어를 수행한다. 고주파 처리는, 블루투스과 같은 통신 환경에서 데이터를 송수신하고자 하는 장치간에 고주파(RF) 통신을 가능하게 하기 위한 것으로, 고주파 신호들의 동기화 및 비트를 심볼(symbol)로 변환하는 기능 등을 포함한다. 베이스 밴드 제어 기능은 부호화/암호화(coding/ciphering), 패킷 핸들링(packet handling), 주파수 호핑(hopping) 등의 기능을 포함한다.

이와 같이 구성된 인증요구 개시측(100)과 인증요구 수신측(110)은 해당되는 호스트의 요구에 의해 상호간의 고주파 동기를 일치시킨 후, 상호간에 연결을 설정하게 된다. 상호간의 연결 설정은 인증요구 개시측(100)과 인증요구 수신측(110)에 각각 구비되어 있는 링크 관리자(106)(116)간의 인증절차를 거쳐 수행된다.

도 2A, B는 본 발명에 따른 인증방법을 수행하는데 있어서, 인증요구 개시측(100)의 동작 흐름도이고, 도 3A, B는 본 발명에 따른 인증방법을 수행하는데 있어서, 인증요구 수신측의 동작 흐름도이다.

도 1, 도 2A, 도 2B, 도 3A 및 도 3B를 참조하여 본 발명에 따른 인증방법에 대해 설명하면 다음과 같다.

먼저, 인증요구 개시측(100)의 링크 관리자(106)가 단계 202에서 종단부(108)를 경유하여 인증요구(Authentication Request) LMP 메시지(LMP_au_rand)를 송출하면, 단계 302에서 인증요구 수신측(110)의 링크 관리자(116)는 종단부(118)를 통해 인증요구 LMP 메시지(LMP_au_rand)를 수신한다.

단계 303에서 링크 관리자(116)는 수신된 인증요구 LMP 메시지(LMP_au_rand)에 대한 인증 응답을 계산한다. 즉, 수신된 인증요구 LMP 메시지(LMP_au_rand)에 포함되어 있는 랜덤(random)정보와 링크 관리자(116)가 보유하고 있는 키(key)정보를 이용한 연산으로 인증 응답을 계산한다. 단계 304에서 링크 관리자(116)는 계산된 인증 응답으로 구성된 인증 응답 LMP 메시지(LMP_sres)를 종단부(118)를 경유하여 인증요구 개시측(100)으로 송출한다.

이에 따라 인증요구 개시측(100)의 링크 관리자(106)는 단계 204에서 종단부(108)를 통해 상술한 인증 응답 LMP 메시지(LMP_sres)를 수신한다. 단계 206에서 링크 관리자(106)는 수신된 인증 응답 LMP 메시지(LMP_sres)가 유효 응답인지를 체크한다. 체크방법은 단계 202에서 송출한 인증요구 LMP 메시지에 포함되어 있는 랜덤(random) 정보와 링크 관리자(106)가 보유하고 있는 키(Key)정보를 이용하여 이루어진다. 즉, 링크 관리자(106)는 자신이 보유하고 있는 키정보와 인증요구 LMP 메시지(LMP_au_rand)에 포함시킨 랜덤정보를 이용한 연산 결과를 링크 관리자(116)로부터 수신한 인증 응답 LMP 메시지(LMP_sres)에 포함되어 있는 인증응답과 비교하여, 현재 수신된 인증응답 LMP 메시지(LMP_sres)가 유효한지를 체크하도록 구현할 수 있다. 이 때, 링크 관리자(106)와 링크 관리자(116)는 동일한 키(key) 정보를 갖는다.

단계 206에서 체크한 결과, 현재 수신된 인증응답 LMP 메시지(LMP_sres)가 유효하지 않으면, 링크 관리자(106)는 해당되는 인증 작업이 실패(fail)한 것으로 판단하고, 단계 208에서 인증에 대한 실패 처리를 한다. 예를 들어, 해당되는 호스트(미 도시됨)측과 인증요구 수신측(110)으로 해당되는 인증작업이 실패되었음을 통보하는 작업을 수행할 수 있다. 그리고, 단계 210에서 해당되는 인증 작업을 종료한다.

그러나, 단계 206에서 체크한 결과, 수신된 인증응답 LMP 메시지(LMP_sres)가 유효한 것으로 판단되면, 링크 관리자(106)는 단계 212에서 현재 연결 설정단계가 초기 접속단계(pairing process)에 해당되는지를 체크한다. 이는 링크 관리자(106)에 구비되어 있는 메모리(105)에 링크 키에 대한 정보가 저장되어 있는지에 따라 결정된다. 즉, 메모리(105)에 링크 키에 대한 정보가 저장되어 있지 않으면, 현재 연결 설정단계는 초기 접속단계로 판단한다.

단계 212에서 체크한 결과, 현재 연결 설정단계가 초기 접속단계에 해당되는 경우에, 단계 206에서 이용한 키는 초기 키(initialize key)정보이다. 따라서, 링크 관리자(106)(116)간에 이용할 링크 키(link key)를 생성하여야 한다. 링크 키는 연결 설정에 의해 링크 관리자(106)(116)간에 형성되는 링크를 인증하는데 사용된다.

이에 따라 현재 연결 설정단계가 상술한 초기 접속단계에 해당되면, 단계 214에서 링크 관리자(106)는 링크 키를 생성하기 위한 LMP 메시지(LMP_comb_key 또는 LMP_unit_key)를 종단부(108)를 경유하여 인증요구 수신측(110)으로 송출하면서 메모리(105)에 저장한다. LMP_comb_key는 링크 관리자(106)가 보유하고 있는 키 정보와 링크 관리자(116)가 보유하고 있는 키 정보를 조합한 결과를 이용하여 링크 키를 생성하고자 할 때 송출되는 LMP 메시지로서, 조합 키(combination key) 생성 요구 메시지이다. LMP_unit_key는 링크 관리자(106)가 보유하고 있는 키 정보만을 이용하여 링크 키 정보를 생성하고자 할 때 송출되는 LMP 메시지로서, 단일 키(unit key) 생성 요구 메시지이다.

단계 214에서 링크 키 생성을 위한 LMP 메시지가 송출되면, 링크 관리자(116)는 단계 308에서 자신의 인증조건을 체크한다. 자신의 인증조건은 상호 인증(Mutual authentication)절차가 고려되어야 하는지를 판단할 수 있는 정보이다. 본 실시 예에서는 인증 인에이블(Authentication_enable) 정보를 이용한다. 예를 들어, 자신의 인증 인에이블정보가 '0x00'으로 설정되어 있으면, 상호인증이 고려될 필요가 없는 것으로 판단한다. 반면, 자신의 인증 인에이블정보가 '0x01'로 설정되어 있으면, 상호인증이 고려될 필요가 있는 것으로 판단한다.

단계 308의 체크결과, 상호인증이 고려될 필요가 없으면, 현재 수신된 LMP 메시지가 링크 생성을 위한 것이므로, 링크 관리자(116)는 단계 309에서 링크 키 생성을 위한 응답 메시지인 LMP 메시지(LMP_comb_key 또는 LMP_unit_key)를 종단부(118)를 경유하여 인증요구 개시측(100)으로 송출한다. 이 때, 송출되는 LMP 메시지는 단계 214에서 송출된 메시지와 관계없이 링크 관리자(106)가 보유하고 있는 키 정보와 링크 관리자(116)가 보유하고 있는 키 정보를 조합한 결과를 이용하여 링크 키 정보를 생성하기 원할 경우에, 조합 키 생성 요구 메시지(LMP_comb_key)가 되고, 링크 관리자(116)가 보유하고 있는 키 정보만을 이용하여 링크 키 정보를 생성하고자 할 때에는 단일 키 생성 요구 메시지(LMP_unit_key)가 된다.

그 다음 링크 관리자(116)는 단계 310에서 링크 키를 생성한다. 링크 관리자(116)는 링크 관리자(106)와 링크 관리자(116)간에 링크 키를 설정하기 위해 송수신한 LMP 메시지가 모두 조합 키 생성 요구 메시지(LMP_comb_key)인 경우에, 조합된 결과에 의존하여 링크 키를 생성한다. 그러나 링크 관리자(106)는 조합 키 생성 요구 메시지(LMP_comb_key)를 송출하였으나 링크 관리자(116)는 단일 키 생성 요구 메시지(LMP_unit_key)를 송출한 경우에, 링크 관리자(116)는 자신의 키 정보에 의존하여 링크 키를 생성한다. 또, 링크 관리자(106)와 링크 관리자(116)간에 송수신한 LMP 메시지가 단일 키 생성 요구 메시지(LMP_unit_key)인 경우에, 링크 관리자(116)는 링크 관리자(106)의 키 정보에 의존하여 링크 키를 생성한다. 이와 같은 기준으로 링크 키가 생성되면, 단계 314에서 초기 접속단계에서의 인증절차를 완료한다.

그러나, 단계 308의 체크결과, 상호인증이 고려될 필요가 있으면, 링크 관리자(116)는 단계 316에서 링크 키 생성을 위해 수신된 LMP 메시지를 메모리(115)에 저장한다. 그 다음, 단계 318에서 링크 관리자(116)는 인증요구 LMP 메시지(LMP_au_rand)를 종단부(118)를 경유하여 인증요구 개시측(100)으로 송출한다.

한편, 링크 관리자(106)는 단계 214에서 링크키 생성을 위한 LMP 메시지를 송출한 후, 단계 216에서 상대방장치인 인증요구 수신측(110)으로부터 LMP 메시지가 수신되면, 단계 218에서 링크 관리자(106)는 수신된 LMP 메시지를 체크한다. 즉, 링크 관리자(106)는 수신된 LMP 메시지가 링크 키 생성을 위한 LMP 메시지(LMP_comb_key 또는 LMP_unit_key)인지 인증요구 LMP 메시지(LMP_au_rand)인지를 체크한다. 체크는 수신된 메시지의 페이로드(payload)에 실려 있는 식별 정보(identification information)(op code)를 이용하여 수행된다. 즉, 링크 관리자(106)는 상술한 식별정보에 의해 현재 수신된 LMP 메시지가 링크 키 생성을 위한 LMP 메시지인지 인증요구 LMP 메시지인지를 판단한다.

단계 218에서 체크한 결과, 현재 수신된 LMP 메시지가 링크 키 생성을 위한 LMP 메시지(LMP_comb_key 또는 LMP_unit_key)이면, 단계 220에서 링크 관리자(106)는 해당되는 링크 키를 생성한다. 이 때, 링크 관리자(106)는 링크 관리자(116)와 링크 키를 설정하기 위해 송수신한 LMP 메시지가 조합 키 생성 요구 메시지(LMP_comb_key)인 경우에, 조합된 결과에 의존하여 링크 키를 생성한다. 그러나 링크 관리자(106)는 조합 키 생성 요구 메시지(LMP_comb_key)를 송출하였으나 링크 관리자(116)는 단일 키 생성 요구 메시지(LMP_unit_key)를 송출한 경우에, 링크 관리자(106)는 링크 관리자(116)의 키 정보에 의존하여 링크 키를 생성한다. 또, 링크 관리자(106)와 링크 관리자(116)간에 송수신한 LMP 메시지가 단일 키 생성 요구 메시지(LMP_unit_key)인 경우에, 링크 관리자(106)는 자신의 키 정보에 의존하여 링크 키를 생성한다. 이와 같은 기준으로 링크 키가 생성되면, 단계 210에서 초기 접속단계에서의 인증 절차를 완료한다.

그러나, 단계 218에서 체크한 결과, 수신된 LMP 메시지가 인증요구 LMP 메시지(LMP_au_rand)이면, 링크 관리자(106)는 단계 222에서 그에 대한 인증응답 LMP 메시지를 종단부(108)를 경유하여 인증요구 수신측(110)으로 송출한다.

이에 따라 인증요구 수신측(110)의 링크 관리자(116)는 단계 320에서 인증응답 LMP 메시지(LMP_sres)를 수신한다. 그 다음, 단계 322에서 링크 관리자(116)는 수신된 인증응답 메시지가 유효한 지를 체크한다. 체크방식은 상술한 단계 206에서와 동일한 방식으로 이루어진다. 단계 322에서 체크한 결과, 수신된 인증응답 메시지가 유효하지 않으면, 링크 관리자(116)는 단계 324에서 인증 실패처리를 하고, 단계 314에서 작업을 종료한다. 인증 실패처리는 단계 208에서와 동일하게 수행된다.

그러나, 단계 322에서 체크한 결과, 수신된 인증응답 LMP 메시지가 유효한 경우에, 링크 관리자(116)는 현재 처리가 링크 키 생성을 위한 LMP 메시지 수신에 따른 것이므로, 단계 325에서 메모리(115)에 저장되어 있는 링크 키 생성을 위한 LMP 메시지에 대응하는 응답 메시지에 해당되는 LMP 메시지를 종단부(118)를 통해 인증요구 개시측(100)으로 송출한다. 그리고, 단계 326에서 링크 관리자(116)는 상술한 단계 310에서와 같이 링크 키를 생성하고, 단계 314에서 초기 접속단계에서의 상호인증 절차를 종료한다.

인증요구 개시측 링크 관리자(106)는 단계 224에서 링크 키 생성을 위한 응답 메시지인 LMP 메시지가 수신되면, 단계 225에서 수신된 LMP 메시지가 단계 214에서 저장한 메시지에 대응되는 응답 메시지인지를 체크한다. 체크결과, 대응되는 응답 메시지인 경우에, 링크 관리자(106)는 단계 226에서 상술한 단계 220에서와 같이 링크 키를 생성한 뒤, 단계 210에서 초기 접속단계에서의 상호인증 절차를 종료한다. 그러나, 단계 225에서 체크한 결과, 수신된 LMP 메시지가 대응되는 응답 메시지가 아니면, 대응되는 응답 메시지가 수신될 때까지 기다린다.

한편, 단계 212에서 링크 관리자(106)가 체크한 결과, 현재의 연결 설정단계가 초기 접속단계가 아니면, 단계 228에서 링크 관리자(106)는 연결(connection) 설정 완료 메시지(LMP_setup_complete)에 해당되는 LMP 메시지를 인증요구 수신측(110)으로 송출하면서 메모리(105)에 저장한다.

이에 따라 링크 관리자(116)는 단계 306에서 연결 설정 완료 메시지에 해당되는 LMP 메시지(LMP_setup_complete)를 수신하게 되어, 단계 308에서 상술한 바와 같이 자신의 인증조건을 체크하게 된다. 체크결과, 상호인증이 필요하지 않은 경우에, 단계 311에서 링크 관리자(116)는 수신된 LMP 메시지에 대한 응답 메시지에 해당되는 연결 설정 완료 LMP 메시지(LMP_setup_complete)를 인증요구 개시측(100)으로 송출하고, 단계 312에서 인증 절차를 종료하고 해당되는 연결을 설정한 뒤, 단계 314에서 연결 설정 작업을 종료한다.

그러나, 링크 관리자(116)는 단계 308의 체크결과, 상호인증이 필요한 경우에 단계 316에서 수신된 연결 설정 완료 LMP 메시지(LMP_setup_complete)를 메모리(115)에 저장한다. 단계 318에서 링크 관리자(116)는 인증요구 LMP 메시지(LMP_auth_rand)를 인증요구 개시측(100)으로 송출한다.

링크 관리자(106)는 단계 230에서 상대 장치인 인증요구 수신측(110)으로부터 LMP 메시지가 수신되면, 단계 232에서 수신된 메시지가 인증요구 LMP 메시지(LMP_auth_rand)인지, 연결 설정 완료 LMP 메시지(LMP_setup_complete)인지를 체크한다. 체크방식은 단계 218에서와 동일하게 이루어진다.

단계 232에서 체크한 결과, 수신된 메시지가 연결 설정 완료 LMP 메시지이면, 링크 관리자(106)는 단계 235에서 인증 절차를 완료하고, 해당되는 연결을 설정한 후, 단계 210에서 연결 설정작업을 종료한다. 그러나, 단계 232에서 체크한 결과, 수신된 LMP 메시지가 인증요구 LMP 메시지(LMP_auth_rand)이면, 링크 관리자(106)는 단계 236에서 그에 대한 인증응답 메시지를 인증요구 수신측(110)으로 송출한다.

링크 관리자(116)는 단계 320에서 인증응답 LMP 메시지가 수신되면, 단계 322에서 상술한 바와 같이 수신된 인증응답 LMP 메시지가 유효한 지를 체크한다. 단계 322에서 체크한 결과, 수신된 인증응답 LMP 메시지가 유효하지 않으면, 링크 관리자(116)는 단계 324를 수행한다. 그러나, 수신된 인증응답 LMP 메시지가 유효하면, 링크 관리자(116)는 단계 327에서 메모리(115)에 저장되어 있는 연결 설정완료 메시지에 대응되는 응답 메시지인 연결 설정 완료 LMP 메시지(LMP_setup_complete)를 인증요구 개시측(100)으로 송출한다. 그리고, 링크 관리자(116)는 단계 328에서 상호 인증 절차를 완료하고, 해당되는 연결을 설정한 뒤, 단계 314에서 연결 설정 작업을 종료한다.

링크 관리자(106)는 단계 238에서 연결 설정 완료 LMP 메시지가 수신되면, 단계 239에서 상술한 단계 228에서 메모리(105)에 저장한 LMP에 대응되는 응답 메시지인지 체크한다. 체크결과, 대응되는 응답 메시지인 경우에, 단계 240에서 링크 관리자(106)는 상호 인증절차를 완료하고, 해당되는 연결을 설정한 후, 단계 210에서 연결 설정 작업을 종료한다.

그러나, 단계 239에서 체크한 결과, 대응되는 응답 메시지가 아닌 경우에, 링크 관리자(106)는 대응되는 응답 메시지가 수신될 때까지 기다린다.

도 4A는 초기 접속(pairing)단계에서 수행되는 인증 절차도에 대한 개념도로서, 단일 인증에 의한 경우이다. 따라서, 도

4A에 도시된 바와 같이, 인증요구 개시측(100)의 링크 관리자(106)에 대한 인증 인에이블(Authentication_Enable)은 "0x01"로 설정되어 있고, 인증요구 수신측(110)의 링크 관리자(116)에 대한 인증 인에이블(Authentication_Enable)은 "0x00"으로 설정되어 있다.

이와 같이 인증 인에이블이 설정된 상태에서, 인증요구 개시측(100)의 링크 관리자(106)가 인증요구 수신측(110)의 링크 관리자(116)로 인증요구 LMP 메시지(LMP_au_rand)를 송출하면, 인증요구 수신측(110)의 링크 관리자(116)는 그에 대한 응답 메시지에 해당되는 인증 응답 LMP 메시지(LMP_sres)를 인증요구 개시측(100)의 링크 관리자(106)로 송출한다.

이에 따라 인증요구 개시측(100)의 링크 관리자(106)는 링크 키를 생성하기 위한 LMP 메시지(LMP_comb_key 또는 LMP_unit_key)를 인증요구 수신측(110)의 링크 관리자(116)로 송출하면서, 송출한 LMP 메시지를 메모리(105)에 저장한다. 인증요구 수신측(110)의 링크 관리자(116)는 링크 키를 생성하기 위한 LMP 메시지(LMP_comb_key 또는 LMP_unit_key)가 수신되면, 그에 대한 응답 메시지에 해당되는 링크 키를 생성하기 위한 LMP 메시지(LMP_comb_key 또는 LMP_unit_key)를 인증요구 개시측(100)의 링크 관리자(106)로 송출하고, 해당되는 링크 키를 생성한 뒤, 초기 접속 단계에서의 인증 절차를 종료한다. 인증요구 개시측(100)의 링크 관리자(106)는 링크 키를 생성하기 위한 LMP 메시지(LMP_comb_key 또는 LMP_unit_key)가 수신되면, 해당되는 링크 키를 생성하고, 초기 접속단계에서의 인증 절차를 종료한다.

도 4B는 초기 접속(pairing)단계에서 수행되는 인증 절차도에 대한 개념도로서, 상호 인증이 필요한 경우이다. 따라서, 도 4B에 도시된 바와 같이, 인증요구 개시측(100)의 링크 관리자(106)와 인증요구 수신측(110)의 링크 관리자(116)에 대한 인증 인에이블(Authentication_Enable)은 모두 "0x01"로 설정되어 있다.

이와 같이 인증 인에이블이 설정된 상태에서, 인증요구 개시측(100)의 링크 관리자(106)가 인증요구 수신측(110)의 링크 관리자(116)로 인증요구 LMP 메시지(LMP_au_rand)를 송출하면, 인증요구 수신측(110)의 링크 관리자(116)는 그에 대한 응답 메시지에 해당되는 인증 응답 LMP 메시지(LMP_sres)를 인증요구 개시측(100)의 링크 관리자(106)로 송출한다.

이에 따라 인증요구 개시측(100)의 링크 관리자(106)는 링크 키를 생성하기 위한 LMP 메시지(LMP_comb_key 또는 LMP_unit_key)를 인증요구 수신측(110)의 링크 관리자(116)로 송출하면서, 송출한 LMP 메시지를 메모리(105)에 저장한다.

인증요구 수신측(110)의 링크 관리자(116)는, 자신의 인증 인에이블이 상호 인증이 요구되는 값으로 설정되어 있으므로, 링크 키를 생성하기 위한 LMP메시지(LMP_comb_key 또는 LMP_unit_key)가 수신되면, 메모리(115)에 저장한다. 그 다음, 인증요구 LMP 메시지(LMP_au_rand)를 인증요구 개시측(100)의 링크 관리자(106)로 송출한다.

인증요구 개시측(100)의 링크 관리자(106)는 링크 키를 생성하기 위한 LMP 메시지를 송출한 상태에서 인증요구 수신측(110)의 링크 관리자(116)로부터 인증요구 LMP 메시지(LMP_au_rand)가 수신되면, 그에 대한 응답 메시지에 해당되는 인증 응답 LMP 메시지(LMP_sres)를 인증요구 수신측(110)의 링크 관리자(116)로 송출한다.

인증요구 수신측(110)의 링크 관리자(116)는 인증응답 LMP 메시지(LMP_sres)가 수신되면, 메모리(115)에 저장하였던 링크 키 생성을 위한 LMP 메시지에 대응되는 응답 메시지인 LMP 메시지(LMP_comb_key 또는 LMP_unit_key)를 인증요구 개시측(100)의 링크 관리자(106)로 송출한 뒤, 해당되는 링크 키를 생성하고 초기 접속단계에서의 상호 인증 절차를 종료한다. 인증요구 개시측(100)의 링크 관리자(106)는 링크 키 생성을 위한 LMP 메시지에 대응되는 응답 LMP 메시지가 수신되면, 해당되는 링크 키를 생성하고, 초기 접속 단계에서의 상호 인증 절차를 종료한다.

도 5A는 링크 키가 생성된 후, 연결 설정을 위한 인증 절차도에 대한 개념도로서, 단일 인증에 의한 경우이다. 따라서, 도 5A에 도시된 바와 같이, 인증요구 개시측(100)의 링크 관리자(106)에 대한 인증 인에이블(Authentication_Enable)은 "0x01"로 설정되어 있고, 인증요구 수신측(110)의 링크 관리자(116)에 대한 인증 인에이블(Authentication_Enable)은 "0x00"으로 설정되어 있다.

이와 같이 인증 인에이블이 설정된 상태에서, 인증요구 개시측(100)의 링크 관리자(106)가 인증요구 수신측(110)의 링크 관리자(116)로 인증요구 LMP 메시지(LMP_au_rand)를 송출하면, 인증요구 수신측(110)의 링크 관리자(116)는 그에 대한 응답 메시지에 해당되는 인증 응답 LMP 메시지(LMP_sres)를 인증요구 개시측(100)의 링크 관리자(106)로 송출한다.

이에 따라 인증요구 개시측(100)의 링크 관리자(106)는 연결 설정 완료 LMP 메시지(LMP_setup_complete)를 인증요구

수신측(110)의 링크 관리자(116)로 송출하면서, 송출한 연결 설정 완료 LMP 메시지(LMP_setup_complete)를 메모리(105)에 저장한다. 인증요구 수신측(110)의 링크 관리자(116)는 연결 설정 완료 LMP 메시지(LMP_setup_complete)가 수신되면, 그에 대한 응답 LMP 메시지(LMP_setup_complete)를 인증요구 개시측(100)의 링크 관리자(106)로 송출하면서, 인증 절차를 완료하고 해당되는 연결을 설정한다. 인증요구 개시측(100)의 링크 관리자(106)는 상술한 응답 LMP 메시지(LMP_setup_complete)가 수신되면, 인증 절차를 완료하고, 해당되는 연결을 설정한다.

도 5B는 링크 키가 생성된 후, 연결 설정을 위한 인증 절차도에 대한 개념도로서, 상호 인증이 필요한 경우이다. 따라서, 도 5B에 도시된 바와 같이, 인증요구 개시측(100)의 링크 관리자(106)와 인증요구 수신측(110)의 링크 관리자(116)에 대한 인증 인에이블(Authentication_Enable)은 모두 "0x01"로 설정되어 있다.

이와 같이 인증 인에이블이 설정된 상태에서, 인증요구 개시측(100)의 링크 관리자(106)가 인증요구 수신측(110)의 링크 관리자(116)로 인증요구 LMP 메시지(LMP_auth_req)를 송출하면, 인증요구 수신측(110)의 링크 관리자(116)는 그에 대한 응답 메시지에 해당되는 인증 응답 LMP 메시지(LMP_auth_rsp)를 인증요구 개시측(100)의 링크 관리자(106)로 송출한다.

이에 따라 인증요구 개시측(100)의 링크 관리자(106)는 연결 설정 완료 LMP 메시지(LMP_setup_complete)를 인증요구 수신측(110)의 링크 관리자(116)로 송출하면서, 송출한 연결 설정 완료 LMP 메시지(LMP_setup_complete)를 메모리(105)에 저장한다. 인증요구 수신측(110)의 링크 관리자(116)는, 자신의 인증 인에이블이 상호 인증이 요구되는 값으로 설정되어 있으므로, 연결 설정 완료 LMP 메시지(LMP_setup_complete)가 수신되면, 수신된 LMP 메시지를 메모리(115)에 저장한다. 그리고, 인증요구 LMP 메시지(LMP_auth_req)를 인증요구 개시측(100)의 링크 관리자(106)로 송출한다.

인증요구 개시측(100)의 링크 관리자(106)는 연결 설정 완료 LMP 메시지(LMP_setup_complete)를 송출한 상태에서 인증요구 수신측(110)의 링크 관리자(116)로부터 인증요구 LMP 메시지(LMP_auth_req)가 수신되면, 그에 대한 응답 메시지에 해당되는 인증 응답 LMP 메시지(LMP_auth_rsp)를 인증요구 수신측(110)의 링크 관리자(116)로 송출한다.

인증요구 수신측(110)의 링크 관리자(116)는, 인증 응답 LMP 메시지(LMP_auth_rsp)가 수신되면, 메모리(115)에 저장하였던 연결 설정 완료 LMP 메시지(LMP_setup_complete)에 대응되는 응답 메시지인 LMP 메시지(LMP_setup_complete)를 인증요구 개시측(100)의 링크 관리자(106)로 송출한 뒤, 상호 인증 절차를 종료하면서 연결을 설정한다. 인증요구 개시측(100)의 링크 관리자(106)는 메모리(105)에 저장되어 있는 연결 설정 완료 LMP 메시지(LMP_setup_complete)에 대응되는 응답 LMP 메시지(LMP_setup_complete)가 수신되면, 상호 인증 절차를 종료하고, 연결을 설정한다.

상술한 링크 관리자간의 연결 설정을 위한 인증방법은 인증요구 개시측(100) 및 인증요구 수신측(110)이 해당되는 호스트(미 도시됨)와 통합된 구조로 구현된 경우에도 적용될 수 있다.

발명의 효과

상술한 바와 같이 본 발명은 블루투스과 같은 통신 규격을 이용하는 통신환경에서 운영되는 장치간에 연결을 설정할 때, 수신측의 인증조건을 고려하여 송수신 링크 관리자간의 인증절차를 수행하는 방법을 제공함으로써, 블루투스과 같은 통신 규격을 토대로 운영되는 통신 환경에서 좀더 신뢰성 있고 정확한 연결 설정 결과를 얻을 수 있는 효과가 있다.

(57)청구의 범위

청구항1

무선으로 데이터를 송수신할 수 있는 장치간의 연결을 설정하기 위한 인증 방법에 있어서,

- (a)상기 연결 설정을 원하는 상대 장치와의 인증절차를 수행하기 위해 상기 상대 장치측으로 제 1 인증요구 메시지를 송출하는 단계;
- (b)상기 제 1 인증요구 메시지에 대한 인증 응답 메시지가 수신되면, 현재의 동작모드에 따른 소정의 메시지를 상기 상대 장치로 송출하면서 저장하는 단계;
- (c)상기 (b)단계 수행 후, 상기 상대 장치로부터 제 1 메시지가 수신되면, 상기 제 1 메시지가 상기 소정의 메시지에 대응되는 응답 메시지인지를 체크하는 단계;
- (d)상기 (c)단계의 체크결과, 상기 제 1 메시지가 상기 응답 메시지가 아니고, 제 2 인증요구 메시지이면, 상기 제 2 인증요구 메시지에 대응되는 응답 메시지를 상기 상대 장치로 송출하는 단계;
- (e)상기 (d)단계 수행 후, 상기 상대 장치로부터 제 2 메시지가 수신되면, 상기 제 2 메시지가 상기 소정의 메시지에 대응되는 응답 메시지인지를 체크하는 단계;

(f)상기 (e)단계 체크결과, 상기 제 2 메시지가 상기 소정의 메시지에 대응되는 응답 메시지이면, 상기 인증절차를 완료하는 단계를 포함하는 것을 특징으로 하는 장치간의 연결 설정을 위한 인증 방법.

청구항2

제 1 항에 있어서,

상기 (b) 단계는,

상기 현재의 동작 모드가 초기 접속 단계이면, 링크 키 설정을 위한 메시지를 상기 소정의 메시지로서 송출하면서 저장하고, 상기 현재의 동작 모드가 상기 초기 접속 단계가 아니면 연결 설정 완료 메시지를 상기 소정의 메시지로서 송출하면서 저장하고;

상기 (f)단계는,

(f1)상기 현재의 동작 모드가 상기 초기 접속 단계이면, 상기 인증절차를 완료하기 전에 링크 키를 생성하는 단계를 더 포함하고,

(f2)상기 현재의 동작모드가 상기 초기 접속 단계가 아니면, 상기 인증절차를 완료하면서 상기 상대 장치 측과의 연결을 설정하는 단계를 더 포함하는 것을 특징으로 하는 장치간의 연결 설정을 위한 인증 방법.

청구항3

제 1 항에 있어서, 상기 (b)단계는,

(b1)상기 인증 응답 메시지가 수신되면, 보유하고 있는 키 정보와 상기 제 1 인증요구 메시지 송출시 이용한 랜덤 정보를 이용하여 상기 인증 응답 메시지가 유효한 지를 체크하는 단계;

(b2)상기 (b1)단계의 체크결과, 상기 인증 응답 메시지가 유효하지 않으면, 인증 실패처리를 하는 단계를 더 포함하는 것을 특징으로 하는 장치간 연결 설정을 위한 인증 방법.

청구항4

제 1 항에 있어서, 상기 인증 방법은,

(g)상기 (c)단계의 체크결과, 상기 제 1 메시지가 상기 소정의 메시지에 대응되는 응답 메시지이면, 상기 인증절차를 완료하는 단계를 더 포함하는 것을 특징으로 하는 장치간 연결 설정을 위한 인증 방법.

청구항5

제 4 항에 있어서, 상기 (b) 단계는,

상기 현재의 동작 모드가 상기 초기 접속 단계이면, 링크 키 설정을 위한 메시지를 상기 소정의 메시지로서 송출하면서 저장하고, 상기 현재의 동작 모드가 상기 초기 접속 단계가 아니면 연결 설정 완료 메시지를 상기 소정의 메시지로서 송출하면서 저장하고;

상기 (g)단계는,

(g1)상기 현재의 동작 모드가 상기 초기 접속 단계이면, 상기 인증절차를 완료하기 전에 링크 키를 생성하는 단계를 더 포함하고,

(g2)상기 현재의 동작모드가 상기 초기 접속 단계가 아니면, 상기 인증절차를 완료하면서 상기 상대 장치 측과의 연결을 설정하는 단계를 더 포함하는 것을 특징으로 하는 장치간의 연결 설정을 위한 인증 방법.

청구항6

무선으로 데이터를 송수신할 수 있는 장치간의 연결을 설정하기 위한 인증 방법에 있어서,

(a)상기 연결 설정을 원하는 상대 장치로부터 인증 절차를 수행하기 위한 제 1 인증요구 메시지가 수신되면, 상기 제 1 인증요구 메시지에 대응되는 응답 메시지를 송출하는 단계;

(b) 상기 (a) 단계 수행후, 상기 상대 장치로부터 소정의 메시지가 수신되면, 자신의 인증 조건을 체크하는 단계;

(c)상기 자신의 인증 조건을 체크한 결과, 상호 인증이 필요하면, 상기 소정의 메시지를 저장하고, 제 2 인증요구 메시지를 상기 상대 장치로 송출하는 단계;

(d)상기 (c)단계 수행후, 상기 상대 장치로부터 상기 제 2 인증요구 메시지에 대응되는 응답 메시지가 수신되면, 상기 (c) 단계에서 저장한 메시지에 대응되는 응답 메시지를 상기 상대 장치로 송출하면서 상기 인증 절차를 완료하는 단계를 포함하는 장치간 연결 설정을 위한 인증 방법.

청구항7

제 6 항에 있어서, 상기 (d) 단계는,

상기 (b)단계에서 수신된 상기 소정의 메시지가 링크 키 생성을 위한 메시지이면, 링크 키 생성을 위한 메시지에 대응되는 응답 메시지를 상기 상대 장치로 송출하고, 링크 키를 생성한 뒤, 상기 인증 절차를 완료하고,

상기 (b)단계에서 수신된 상기 소정의 메시지가 연결 설정 완료 메시지이면, 상기 연결 설정 완료 메시지에 대응되는 응답 메시지를 상기 상대 장치로 송출하고, 상기 인증 절차를 완료한 후, 상기 상대 장치와의 연결을 설정하는 것을 특징으로 하는 장치간 연결 설정을 위한 인증 방법,

청구항8

제 6 항에 있어서, 상기 (d)단계는,

(d1)상기 제 2 인증요구 메시지에 대응되는 응답 메시지가 수신되면, 상기 제 2 인증요구 메시지를 송출할 때 이용한 랜덤 정보와 보유하고 있는 키 정보를 이용하여 상기 제 2 인증요구 메시지에 대응되는 응답 메시지가 유효한지를 체크하는 단계;

(d2)상기 (d1)단계의 체크결과, 상기 응답 메시지가 유효하지 않으면, 인증 실패처리를 하는 단계를 더 포함하는 것을 특징으로 하는 장치간의 연결 설정을 위한 인증 방법.

청구항9

제 6 항에 있어서, 상기 (b)단계는 인증 인에이블 정보를 상기 인증 조건으로서 체크하는 것을 특징으로 하는 장치간의 연결 설정을 위한 인증 방법.

청구항10

무선으로 데이터를 송수신할 수 있는 장치간의 연결을 설정하기 위한 인증 방법에 있어서,

상기 데이터를 송수신할 수 있는 장치 중 인증 요구를 수신하는 장치에 설정되어 있는 인증조건에 따라 데이터 송수신을 원하는 장치간의 상기 연결 설정을 위한 인증절차를 단일 인증 절차로 수행할 것인지 상호 인증절차로 수행할 것인지를 결정하여 수행하는 단계를 포함하는 장치간의 연결 설정을 위한 인증 방법.

청구항11

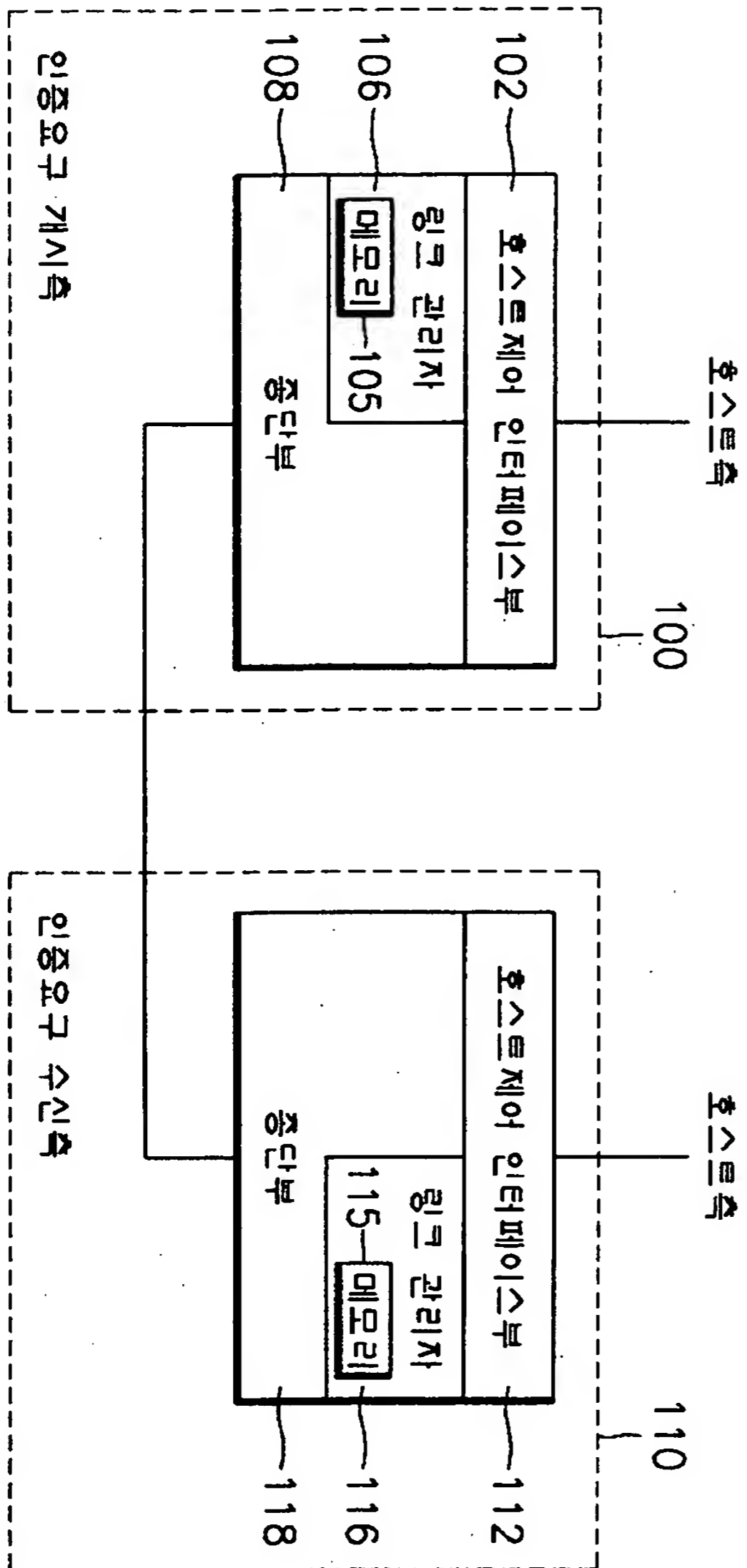
제 10 항에 있어서, 상기 인증절차를 수행하는 단계는 상기 인증 요구를 수신하는 장치에 설정되어 있는 인증조건이 상기 상호 인증절차가 필요한 것으로 설정되어 있으면, 인증을 요구하는 장치측으로 인증 요구 메시지를 송출하여 상기 상호 인증절차를 수행하는 것을 특징으로 하는 장치간의 연결 설정을 위한 인증 방법.

청구항12

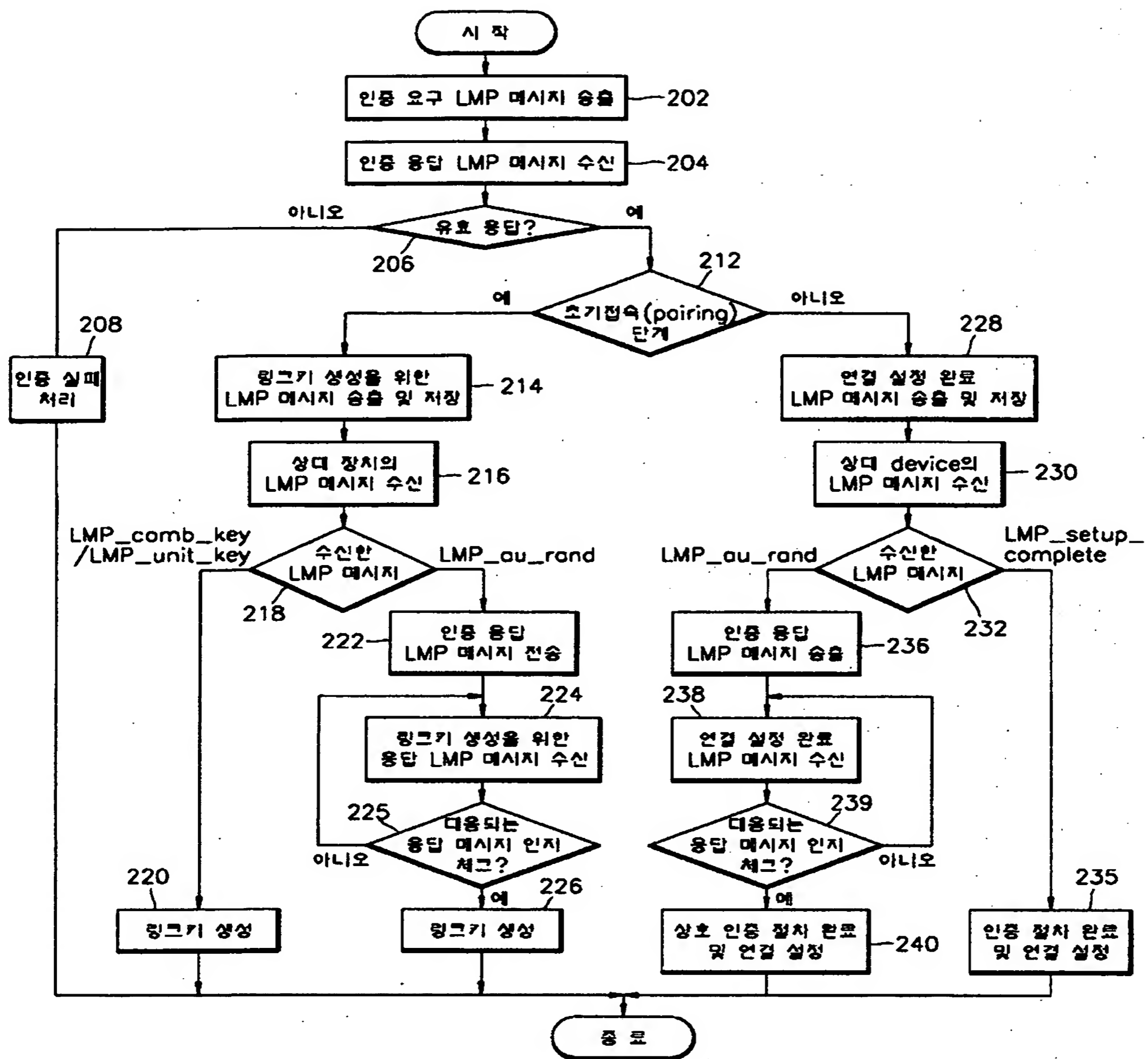
제 10 항에 있어서, 상기 인증절차를 수행하는 단계는 상기 인증 요구를 수신하는 장치에 설정되어 있는 인증 인에이블 정보를 체크하여 해당되는 인증절차를 결정하는 것을 특징으로 하는 장치간의 연결 설정을 위한 인증 방법.

도면

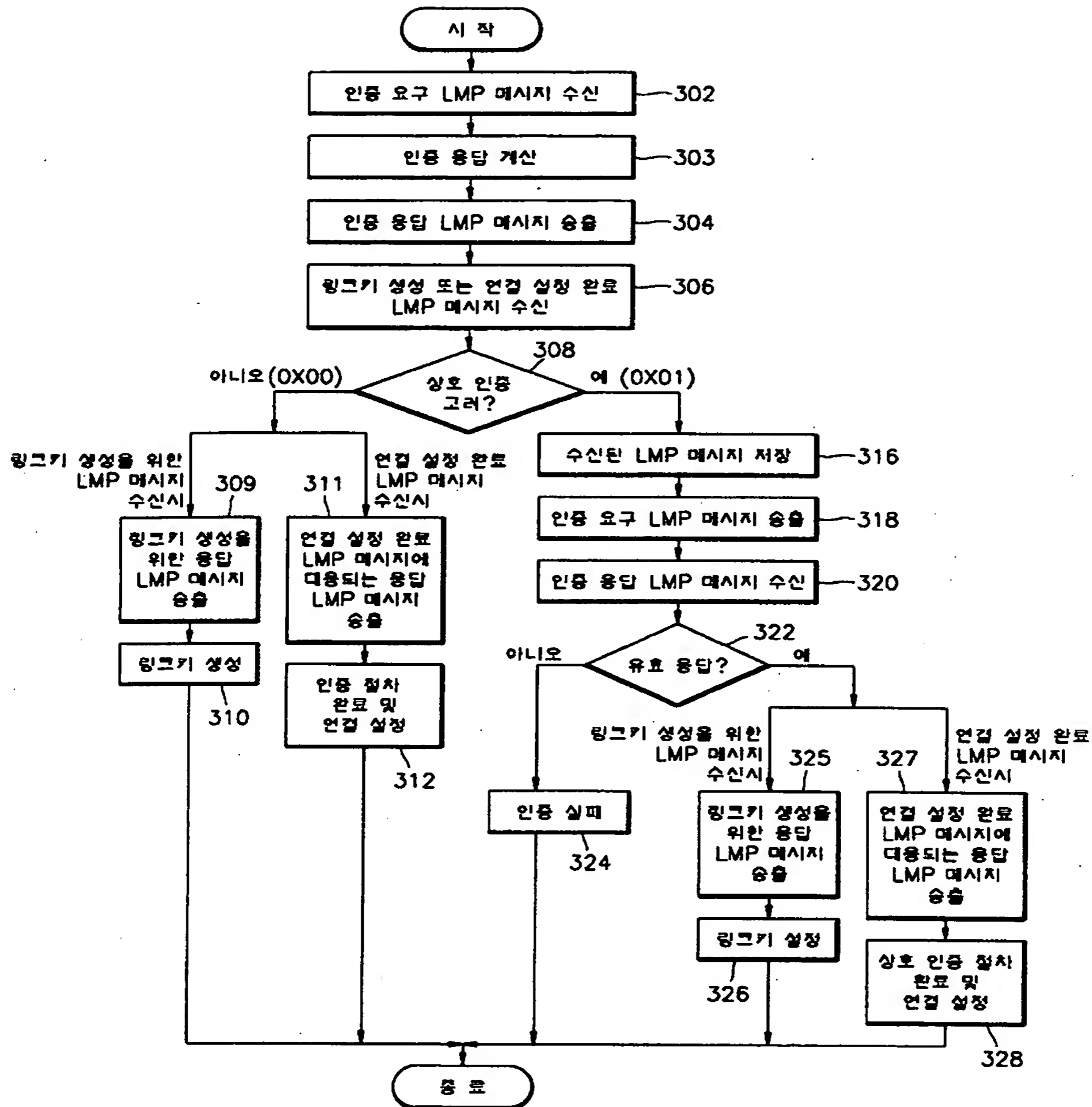
도면1



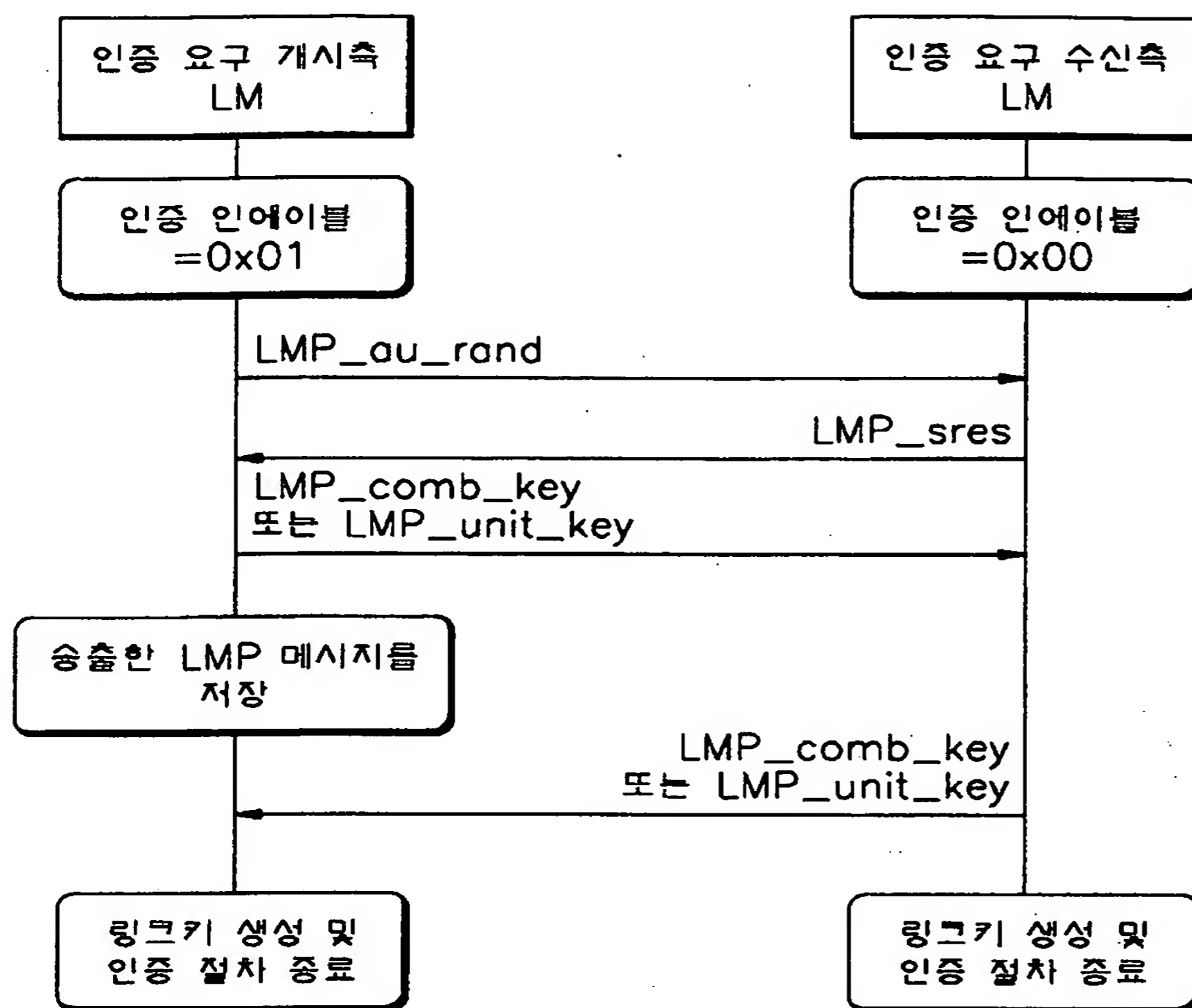
도면2



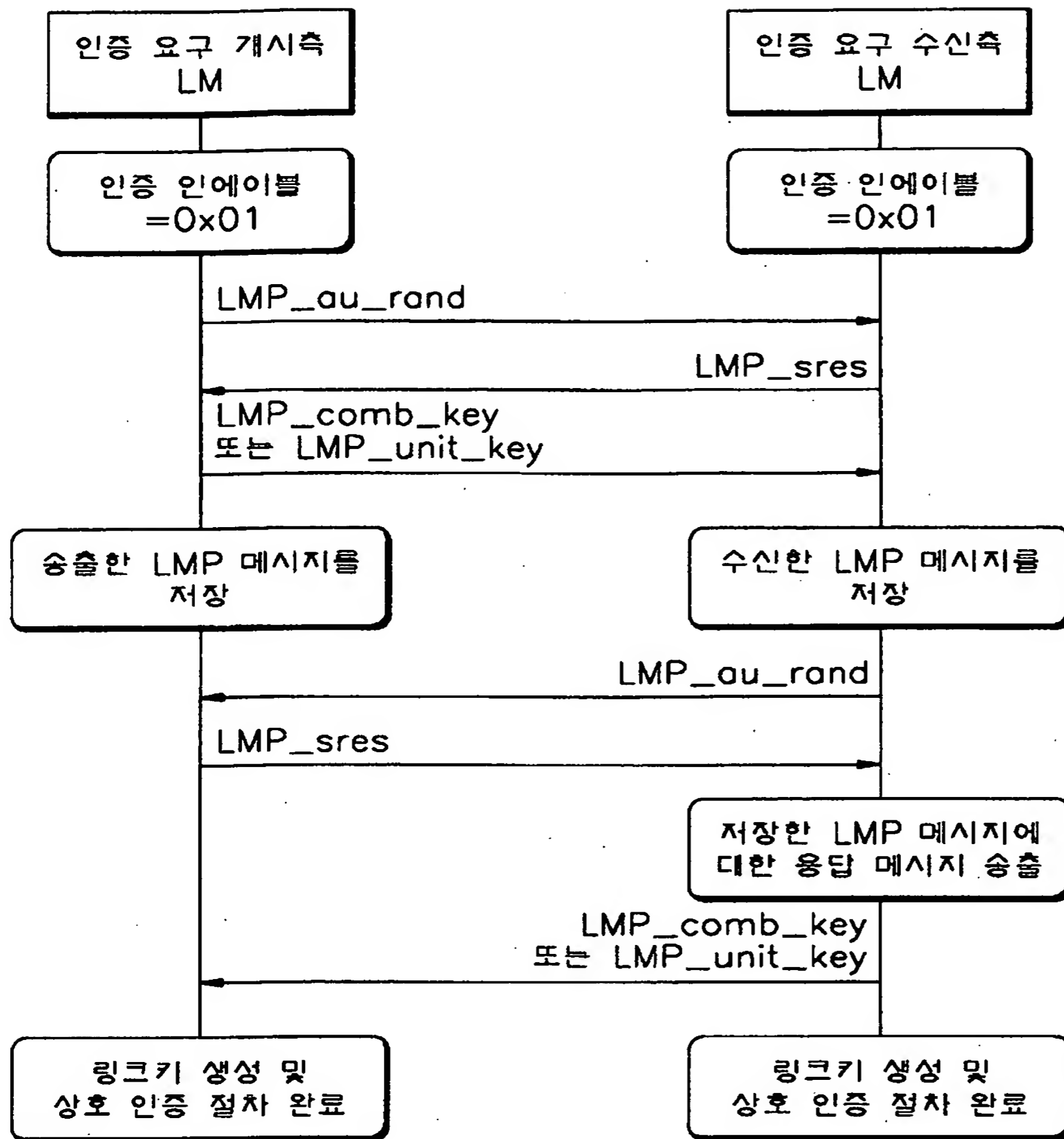
도면3



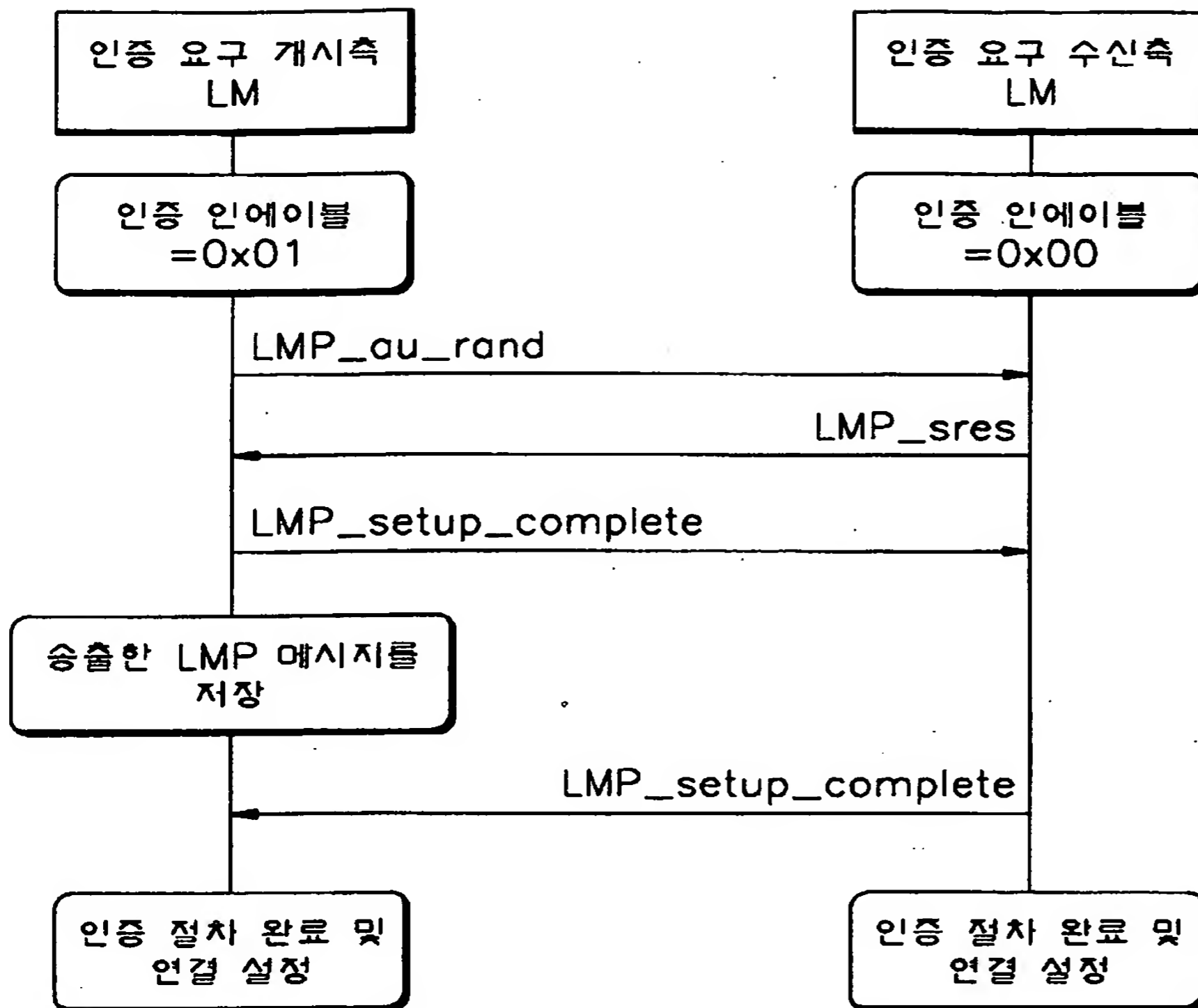
도면4a



도면4b



도면5a



도면5b

